WIRELESS WORLD
RESEARCH FORUM

A Proposal for Self-Organizing Personal Networks

L. Muñoz, L. Sanchez, J. Lanza[1)], M. Alutoin, S. Lehtonen[2)], D. Zeghlache, M. Girot Genet, W. Louati[3)], J. Hoebeke, I. Moerman, G. Holderbeke[4)], M. Ghader[5)], M. Jacobsson[6)]

[1)] Univ. of Cantabria (Spain), [2)] VTT (Finland), [3)] INT (France), [4)] IMEC (Belgium), [5)] University of Surrey (U.K), [6)] Delft University of Technology (The Netherlands).

Personal Network (PN) is an emerging concept which combines pervasive computing and strong user focus. The idea is that the user's personal devices organize themselves in a secure and private personal network transparently of their geographical location. This paper studies a PN architecture where devices form clusters using shared key cryptography over short range radio links on an ad hoc manner and where the otherwise isolated clusters are interconnected over the IP infrastructure using dynamic tunneling. This paper describes work undertaken in the context of the FP6-IST-IP-507102 'My personal Adaptive Global Net' IST-MAGNET project. MAGNET is a worldwide R&D project within Mobile & Wireless Communication beyond 3G

Index Terms—**Cluster, Personal Network, Private Personal Area Network, Self-configuration**

Introduction

TAKE the concept of pervasive computing and combine it with strong user focus and you get Personal Networks (PN) [1], [2]. PN is a collection of one's most private devices referred to as personal nodes. From a technical point of view, the PN is seen to consist of devices sharing a common trust relationship. Security and privacy are the fundamental properties of the PN, as well as its ability to self-organize and adapt to mobility and changing network environments.

The IST project MAGNET [3] vision is that Personal Networks (PNs) will support the users' professional and private activities, without being obtrusive and while safeguarding privacy and security [4]. A PN can operate on top of any number of networks that exist for subscriber services or are composed in an ad hoc manner for this particular purpose. These networks are dynamic and diverse in composition, configuration and connectivity depending on time, place, preference and context, as well as resources available and required, and they function in cooperation with all the needed and preferred partners.

Opposite to other initiatives that explore fields like wireless personal area networking [5], mobile ad hoc networks [6] or self-configuration [7], [8] in isolation focusing on optimizing the characteristics of each field without having much in mind about the others. The solution proposed here presents an integrated approach that copes with the different connectivity, networking and service requirements in order to accomplish the aforementioned vision of an autonomous and self-organized secure Personal Network.

Besides the personalization and privacy requirements that are imposed on the Personal Networking paradigm, self-configuration is the main cornerstone for supporting this concept. In this sense, all the personal nodes a user owns must always be ready to provide their services in a transparent way to the user. This paper will

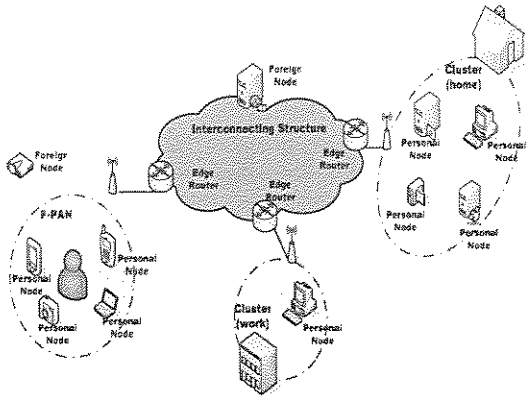


Figure 1: Personal Network architecture and entities

focus on this latter feature by examining the solutions adopted for complete PN formation, from the clusters formation (i.e. how nodes join and leave the cluster) to inter-cluster coordination and communication (i.e. how clusters organize themselves to allow communication between nodes in remote clusters).

The presented solutions have been implemented as components of an integrated proof-of-concept prototype which aims at showing the feasibility of coping with the different challenges that the personal networking concept involves, understood as one of the main contributions of IST-MAGNET project.

Some of the proposed mechanisms have been challenged by other possible ones that have been studied but not integrated in the proof-of-concept prototype (e.g. [9]). A part of the future work will be to compare the different mechanisms studied (i.e. the ones integrated in the prototype and the ones studied in isolation) and optimize the adopted ones with the lessons learned. In order to limit the size of the paper, we will focus on the mechanism that have been implemented and integrated in the proof-of-concept prototype.

The structure of the paper is as follows: in Section II we present the main entities that comprise the proposed architecture, followed by the description of this architecture in Section III. The definition of the mechanisms that cope with the requirements imposed by a self-organized Personal Network is done in Section IV. Section V presents the fundamentals of the implemented proof-of-concept prototype. Finally Section VI concludes the paper and VII discusses future work.

Architectural entities and Terminology

This section presents the main entities that comprise the proposed Personal Network architecture, defining as well, the terminology that will be used in this paper when describing the architecture and the different solutions adopted to support the formation and operation of Personal Networks.

As shown in the Figure 1, the PN consists of clusters of personal nodes. One cluster is special, because it is located around the user. The clusters are connected with each other via an interconnecting structure, which is likely to be infrastructure based. In order to protect the privacy of the user and the integrity of the PN, security measures are used to encrypt the user's data when it is sent outside of the device, i.e. using a wireless medium or the infrastructure. The user can reach all of his or her devices using a variety of underlying networking technologies, which are invisible to the user. The user only sees the services that are available in the PN and on foreign nodes that have been made available to the user.

In this section, the terms and key concepts that are used in the PN architecture will be presented and defined.

- **Device:** Any communicating entity.
- **Node:** A device that implements IPv6 [10] and/or IPv4 [11].
- **Personal Node:** A node related to a given user or person with a pre-established trust attribute. These attributes are typically cryptographic keys with a permanent (as long as not cancelled, redefined or revoked) trust relationship.
- **Private Personal Area Network (P-PAN)/Cluster:** A network of personal devices and nodes, characterized by a common trust relationship, which can communicate with each other without using non-personal nodes. Nodes and devices in a cluster can become members of a P-PAN when a person enters an area where the cluster nodes are located. A P-PAN is often referred to as a personal bubble around a person.
- **Personal Network:** A Personal Network includes the P-PAN and a dynamic collection of remote personal nodes and devices organized in clusters that are connected to each other via

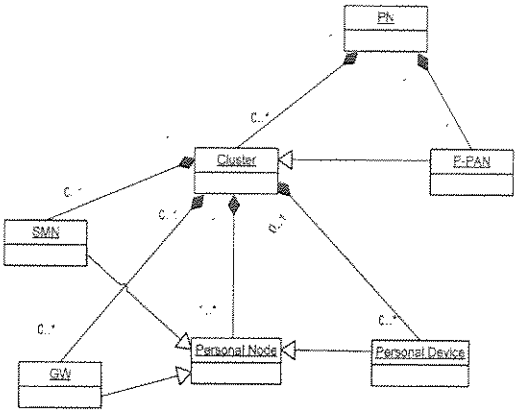


Figure 2: Personal Network principal entities relationships

Interconnecting Structures.

- **Trust Relationship:** is established when two parties communicate and determine with a measure of certainty each other's credentials to set up a secure communication channel using encryption mechanisms. When devices and nodes want to establish a secure communication channel, they build a trust relationship by whatever means possible.
- **Imprinting:** A procedure to bootstrap a trust relationship between two nodes that basically consists of an authenticated key exchange.
- **Gateway Node (GW):** A Personal Node within a Cluster that enables connectivity with the Interconnecting Structures.
- **Interconnecting Structures:** Public, private or shared wired, wireless or hybrid networks such as a UMTS network, the Internet, an intranet or an ad hoc network.
- **Edge Router:** A node in the Interconnecting Structure that communicates with Gateway Nodes and supports them by offering PN functionality.
- **Foreign Node:** A node that is not personal and cannot be part of the PN. Foreign nodes can either be trusted or not trusted. Whenever trusted, they will typically have an ephemeral trust relationship with a node in a PN.

Figure 2 indicates how the PN entities defined in this section relate to each other. Note that, the P-PAN is a materialization of the Cluster concept. The difference between the P-PAN and the rest of the PN Clusters is that the user is in the surroundings. This difference only takes importance on the so called Service Abstraction Level (see Section III). Therefore, in the remainder of the paper we will use both terms without distinction.

Personal Networks Architecture

As shown in Figure 3, the architecture defined within MAGNET presents a layered view where three abstraction levels have been identified. This approach allows detaching the different requirements and challenges that need to be tackled on each of the different abstraction levels.

Going from the bottom up, the first level is the Connectivity Level, which can roughly be mapped onto OSI layers 1 and 2. Here the devices are organized in Radio Domains (RD).

The Network Level, consisting of OSI layers 3, 4 and 5, is placed above the Connectivity Level. The P-PAN and the PN are defined at this level. The P-PAN is a set of personal nodes around the user. The PN further extends the P-PAN concept as a collection of all "my active personal nodes" both remote and in the vicinity of the user. The personal nodes in the PN are grouped in clusters such as: the P-PAN itself, Home cluster, Office cluster, etc. The communication between the different clusters happens via the interconnecting structure over secure dynamic tunnels. The important point in this architecture is the strong focus around the long term trust concept. Only nodes that are able to establish long term trust can be part of the user's P-PAN/PN.

In order to reflect the provision and usage of services in the P-PAN/PN concept, a Service Level is defined above the Network

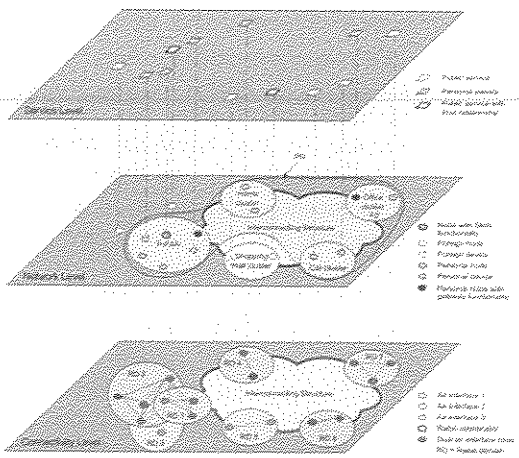


Figure 3: Three abstraction levels view

Level and fills the remaining OSI layers 6 and 7. It contains all the services offered on the nodes/devices in the Network Level. Personal services are offered and used only by personal nodes in PN sense. This implies that these services can be used only if the long term trust relation is established.

Having these abstraction levels in mind the solution presented in this paper has tackled the challenges that appear in each of the abstraction levels in both the Clusters and PN self-configuration.

Personal Networks Self-configuration

Before any specific description of the PN self-configuration mechanisms in the abstraction levels can be presented, a number of basic security notions and concepts must be introduced since privacy and security are the key features that rule the formation of the PN. The MAGNET architecture relies on the notion of long term and short term trust relationships. The long term trust, which could also be perceived as permanent trust, is used to establish a strong security association or relationship between the nodes and devices of the PN. The long term secrets, in fact cryptographic keys, are used to form in essence the trust among the PN constituents, and especially the P-PAN/Cluster components.

These trust relationships are intended to be used between personal nodes owned by the same user. That is to say, the design is based on node ownership, which is a concept easily understood by end users. This is crucial since the end-user understanding of the trust relationship model influences the security of PNs. A lack of understanding of how this works and what consequences it has can jeopardize the security of that person's PN. Nevertheless, while the design is made with ownership in mind, there is nothing in the technical solution that will prevent a user to use the trust relationships in different way. Someone can create long-term trust relationships between nodes of a family for instance.

The long term trust keys are used as a basis to establish communications between Cluster and PN nodes. The process of inserting a given secret in a device or node is referred to as imprinting a device [12]. The goal of imprinting is to establish a long-term trust relation with a new device or node. Long-term trust is mostly established among the PN constituents and is meant to ease the secure formation of the P-PAN and the PN and offer personal and secure services to end users.

Thereby, when introducing a new device to the PN, this device will be paired with at least one other device participating in PN and thus trusted by the other personal nodes. During this procedure the new device will establish a long term pair-wise key with a personal node. This key will be referred to as the PN key in this document. As a result of the pairing procedure, the peers derive a long-term shared key that is subsequently used to secure the communication between them. Each device must store this information securely in the form of a device record. A peer record contains the following information: (1) Peer identifier – a unique identifier associated to the device; (2) PN key – the shared secret derived from the pairing process.

Once the long-term trust between devices and nodes has been established, it is used as a basis to derive long term semi-permanent link layer keys (for use at the connectivity abstraction level) to actually form the P-PAN. Only devices that share the long term trust are allowed to join the P-PAN. The link layer keys are used in turn to establish short session keys, that are dynamic and ephemeral, according to the security framework of each readily available radio or link technology today on the market (or soon to come).

Clusters self-configuration

Opposite to other descriptions of cluster or Personal Area Network [4], [6] that limit the concept to a matter of radio coverage (e.g. 10m range), the concept of cluster proposed in this architecture stands on an opportunistic, distributed, multihop and proactive approach based on the trust relationships established between the cluster constituents. Further, it copes with the heterogeneity support, dynamic adaptation, infrastructureless environment survival and privacy requirements imposed by the P-PAN concept.

In this sense, the clusters will be as large as possible (as long as a new personal node or device is reachable through a PAN air interface, the cluster will add a new wireless hop to its structure), adding new personal

nodes and devices as soon as they appear in the cluster surroundings.

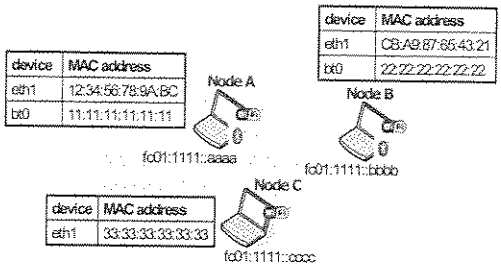
This section presents the mechanisms that coordinately form a PN cluster.

Neighbour discovery and authentication

This is the initial step of the cluster formation. When a personal node is turned on, it needs to find other personal nodes in order to form a Cluster (Cluster formation process). To this end, a personal node will periodically broadcast beacon messages on all its interfaces in order to find other personal nodes in its environment. These packets are the only messages that are sent in clear. This solution can be substituted with air-interface neighbor discovery proprietary mechanisms (i.e. some radio access technologies implement neighbor discovery mechanisms at MAC level), where available, in order to reduce the usage of the wireless channel and the battery consumption. The information in the beacon packet basically consists of a node identifier derived as a digest over the peer's public Diffie Hellman key used during the imprinting procedure (other parameters such as the node IP address are also exchanged in the beacon packets).

Upon the reception of a beacon (or any other way of link layer level peer detection), it will be checked if the node is already registered in the neighbors table; if the peer is already registered, the entry will be updated by reinitializing the expiration timer associated (note that there could be multiple entries for a single identifier, each of them associated with a different interface so as to allocate multimode devices). If the neighbor is not already registered an authentication method will be called in order to assure that the discovered node is really a personal node. It is important to note that each entry is unique by the pair: identifier of the neighbor and interface from which the beacon was received. In this sense, it is required to perform a different authentication process for each of the air interfaces with which is possible to communicate with the neighbor.

The authentication is performed through a three way handshake (Request – Response – Success), that assures a mutual authentication, in which the long-term shared key is used to verify the identity denoted by the identifier field in the beacon received.



Node A Pn Neighbors table

@IP	@MAC	dev	L2 key	BCAST key
fc01:1111::bbbb	CB:A9:87:65:43:21	eth1	454	PNPN
fc01:1111::bbbb	22:22:22:22:22:22	bt0	909	GVGJ
fc01:1111::cccc	33:33:33:33:33:33	eth1	111	CCCC

Node B Pn Neighbors table

@IP	@MAC	dev	L2 key	BCAST key
fc01:1111::aaaa	12:34:56:78:9A:BC	eth1	454	XYXY
fc01:1111::aaaa	11:11:11:11:11:11	bt0	909	QTQT
fc01:1111::cccc	33:33:33:33:33:33	eth1	222	CCCC

Node C Pn Neighbors table

@IP	@MAC	dev	L2 key	BCAST key
fc01:1111::aaaa	12:34:56:78:9A:BC	eth1	111	XYXY
fc01:1111::bbbb	11:11:11:11:11:11	eth1	222	PNPN

Figure 4: P-PAN formation neighbors tables

Besides the authentication process, upon the addition of a new entry, the layer 2 session key generation and exchange procedure will be triggered. During this negotiation process, it is also exchanged the broadcast key of the peers. It is important to note that this procedure will depend on the possibility of both nodes to perform layer 2 encryption. If one of the nodes is not able to encrypt layer 2 frames, the entry in the neighbors table will reflect it and layer 3 encryption (IPSec) must then be provided.

Figure 4 shows an example of which information the nodes would manage after a P-PAN is formed.

In addition to the peer detection, beacons are also used to detect when a node leaves the neighborhood.

On top of this connectivity level neighbor discovery, a MANET-based [6] proactive routing protocol is used in order to complete the Cluster self-configuration at the network abstraction level. Upon the detection/disappearance of the first/last link towards a new personal node, the detection+authentication/deletion mechanism informs the routing protocol about these events. The basics of proactive routing protocols mandate that all nodes in the cluster always maintain a fresh valid route to the rest of the nodes in the cluster.

Thus, the combination of these two mechanisms (i.e. peer detection and proactive routing protocol) allows cluster self-configuration and self-healing behavior.

Additionally, this feature connects with the next section where packet forwarding support is discussed. Note that within a cluster, multihop topologies are possible due to both heterogeneous environments (in terms of air-interfaces) and coverage extension.

Packet forwarding

As has been said, the cluser/P-PAN can be seen as a multihop ad hoc network. In order to overcome the heterogeneity requirement a combined connectivity-network abstraction levels solution has been proposed.

The concept of isolating the upper-layers from underlying wireless technologies and thus providing real multi-mode can be achieved by introducing a Universal Convergence Layer (UCL) [13]. The UCL mainly will act as an enabler for backward and forward compatibility by defining a common interface towards the network layer while managing several different wireless access technologies independently of their PHY and MAC layers. In this sense, the solution adopted, as shown in Figure 4, makes it possible for the nodes to have a single IP address independently of how many air interfaces it has. This way the routing protocol placed in layer 3 will be able to settle routes embracing multiple radio domains in a completely seamless manner.

The combination of these two techniques, UCL plus ad hoc routing protocol, enables managing the heterogeneity that will appear in the P-PAN environment.

This way, the route selection and the packet forwarding is carried out at the network level (i.e. based on the use of an ad hoc routing protocol) while the selection of the optimal (depending on physical and link layer parameters) air interface to use, whenever there are multiple choices, as well as other frame formatting and buffering issues are performed at the UCL.

Additionally, the solutions adopted at the UCL allow feeding the routing protocol with the immediate neighbors of a node independently of the radio domain(s) which both nodes are sharing, thus, optimizing its performance.

In the P-PAN environment, proactive ad hoc routing protocols fit better in the PN architecture; they can react faster to routing requests than reactive protocols, and as has been said, by using some mechanisms (at the connectivity abstraction level), the protocol overhead can be reduced.

Service discovery support

The defined architecture for service discovery within MAGNET specifies [14] a centralized approach within the clusters. One of the nodes in the Cluster will become a Service Management Node (SMN). The role of the SMN is to keep a repository of all provided services within the cluster and the immediate surroundings. In this sense, among all the candidates to take the role of SMN, called Service Assistance Node (SAN), present in a cluster, one has to be selected as the SMN. The election is based on a cost function that includes a combination of values referring to battery status, computing capabilities, network interfaces and database storage capacity. The result of applying this function, from now on called SNW (Service Node Weight), summarizes the nodes' capabilities and is used to identify the most capable one to become the SMN.

In order to select the SMN, each SAN must announce its capabilities, that is, its SNW, and also be aware of those of the other potential SMNs. Thus, some kind of information exchange needs to be established among all SANs within the cluster. In this sense, a protocol data unit has to be defined. This new primitive has to include both the SNW and node's identity. Once the selection procedure is finished, the node that has acquired the role of SMN will announce its presence by sending out an SMN Advertisement, destined to cluster-wide multicast address. These advertisements will be periodically sent to keep the other SANs informed of its presence. Moreover, other nodes will use them to know to whom they have to direct their service discovery queries. Thus, this procedure has a twofold objective of maintaining the SMN role presence among the SANs and informing the cluster nodes about the location of the SMN. In case no SMN is detected during a certain interval, a SAN will start the SMN Challenge procedure to become SMN. This procedure guarantees the continuous presence of a SMN within the cluster.

The service discovery architecture is tightly connected with the Intentional Naming System (INS) [15] naming resolving scheme, providing a flexible and extensible framework called Service Management Layer.

Establishing connectivity with the outer world

Although the P-PAN is an autonomous network that does not need the support of the infrastructure to operate, it is compulsory to be able to establish the means in order to widen the scope of the P-PAN and support the user connectivity with the outer world and the rest of the personal nodes located in remote clusters as soon as it is possible.

The node that is responsible for interconnecting the P-PAN with the outer world is the Gateway node. This node is able to detect its connectivity with the interconnecting infrastructure and dynamically inform this capability by using the mechanisms supported by the ad hoc routing protocol.

Since in proactive routing protocols, each node maintains routing information to the destinations in the local network, the packets to the outside network can be recognised immediately and forwarded to the proper gateway nodes. Besides, the proactive protocols allow the gateway nodes to propagate their advertisement message within its routing updates. In this way, the nodes in the P-PAN can obtain the information of multiple gateways simultaneously, and thus enables smooth handoffs in case of mobility or access network selection (e.g. UMTS vs WiFi hotspot) depending on user preferences or application QoS requirements.

Clusters merging / splitting

We have already presented the mechanisms through which nodes join and leave the clusters as well as the procedures by which special cluster entities (i.e. SMN, GW) are selected and announced. Nevertheless, an important issue that must be solved for having a complete solution tackling cluster self-configuration is the merging of two clusters from the same PN (e.g. the user arriving at home – Home cluster is merged with the P-PAN).

Three main areas are involved when dealing with this problem: the nodes' addressing, the routing information modification and the special entities status.

PN Addressing

The solution adopted for personal nodes' addressing is to use a private address space.

TABLE 1: MAGNET IPV6 ADDRESS FORMAT

48 bits	16 bits	64 bits
PN Prefix	Subnet ID	Interface ID

Personal nodes will have a Unique Local IPv6 Unicast address [16] assigned through the use of a flat addressing scheme as shown in Table 1 where:

- **PN Prefix:** The first byte is taken from the Unique Local IPv6 Unicast address space [16] and the remaining 40 bits (may be unique to each PN) are exchanged during the node imprinting process in order to assure that all personal nodes within a PN share the same PN prefix.
- **Subnet ID:** Bits of the Subnet ID protocol field are 'all zeros', reserved for flat addressing.
- **Interface ID:** The Interface ID is a globally unique identifier which is generated from a 48-bit MAC address as described in Appendix A of [17].

Flat addressing means that the addresses do not provide any hint on the relative location of the personal nodes. In other words, a personal node can have the same address, regardless of where it is attached to the personal network topology. When a node moves from one Cluster to another Cluster of the PN, its address can remain the same, but the routing tables need to be updated for the packets to arrive in the correct part of the PN. Applications that are not capable of dealing with changing IP addresses can work uninterrupted in the flat addressing scheme (provided that handovers are done smoothly). So, the addressing challenge is tackled by using this solution.

Routes modification

It is important to note that the only way to communicate between two personal nodes belonging to two different clusters is through a gateway node and the interconnecting structures. In this sense, when two clusters are merged, all the routes towards the nodes in the other cluster must be reconfigured. As has been said, the routing protocol used for cluster formation and packet forwarding follows a proactive approach that allows that as soon as a node from the first cluster detects the existence of a new node in the surroundings the routing tables are updated accordingly. This information progressively will reach all the nodes of both clusters

revoking the old ones that make use of the interconnecting structures.

Similarly, when a cluster is split in two, the disappearance of the last connecting link will result on the calculation of new routes through the interconnecting structures to connect nodes belonging to the two new clusters.

Cluster special entities status

In the network architecture defined, there are two kind of personal nodes that develop special tasks within the cluster, namely the SMN and the Gateway.

Before analyzing the procedures followed by these nodes during a cluster merge/spilt, it is important to note that several of the networking techniques used, rely on the capacity of involving all the nodes in the P-PAN (or cluster) like the routing protocol updates or most of the service discovery queries, advertisements and SMN selection procedure. In this sense, it is necessary to deploy a mechanism that makes it possible to flood the cluster in a secure manner.

The solution adopted relies on the capacity of each node to perform a secure broadcast transmission (using the broadcast key derived as outlined) and the definition of a cluster-wide multicast address. Whenever a node wants to send a packet that must reach all the nodes within the P-PAN it uses the cluster-wide multicast address. This solution, also known as blind flooding, relies on the security mechanisms implemented at the connectivity level to limit the scope of the flood to the cluster boundaries. Other algorithms under study [18], [19] look for minimizing the overall transmission cost and it is a future analysis work to compare the benefits introduced with the additional complexity.

SMN advertisements are sent to this cluster-wide multicast address so all nodes in the cluster are aware of its presence. When two clusters merge, both SMNs (one from each cluster) will detect the conflict and will challenge each other in order to decide which one is the best choice to take up the role of SMN in the newly formed cluster. Similarly, when a cluster splits, one of the two clusters formed will not have an SMN, those SANs in the cluster that lacks from an SMN will detect this situation and start a challenge to resolve which of them assumes this role in the new cluster.

The status with the Gateways nodes on each of the clusters merging/splitting doesn't change in these situations, as the uniqueness is not compulsory like in the SMN case. Gateway nodes will only need to adjust their routing tables at cluster level, and raise this information to the PN level in order to update the information related to the nodes reachable through it (those on the other cluster in the merging and those that remain near the gateway in the splitting).

PN self-configuration

In order to form the PN and realise inter-Cluster communication over a fixed infrastructure, four requirements need to be fulfilled. First of all, the Clusters need to have access to the fixed infrastructure through one or multiple Gateway Nodes. Secondly, once access to the fixed infrastructure is available, the Clusters need to be capable of locating each other. Thirdly, once they have located each other, they should establish tunnels between them. Last but not least, once the PN has been formed, it should be able to maintain itself in view of dynamics in the network. We will now discuss how these requirements lead to a conceptual PN architecture that relies on the concept of a PN Agent.

The description of the PN Agent based PN establishment is further specialized to the case where edge routers in the infrastructure provide PN support services and naming systems are also available to supplement the overall architecture. This specific case assumes that such new components when compared to existing wireless PANs and infrastructure technologies are readily available or will be introduced in next generation networks.

Connectivity between remote Clusters can only be realised if Clusters can locate each other. The PN Agent concept has been introduced to assist in this localisation and in the overall PN establishment. The PN Agent could be implemented as part of the user's fixed PN Cluster (e.g. the cluster of nodes around the user's home or office). It can also be implemented as a service under the control of service or network providers.

The PN Agent keeps track of each personal node and all Clusters in a PN. Clusters that have connectivity to the infrastructure need to register themselves with the PN Agent. Based on this information, the PN Agent can provide the Clusters with information on the location of other Clusters

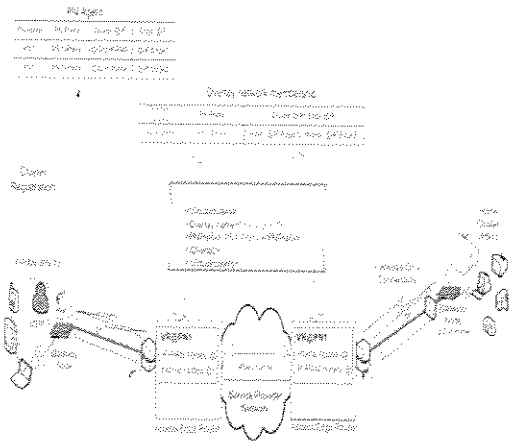


Figure 5: Deployment of tunnels and overlays in the PN Agent based PN establishment

that belong to the PN. This information is indispensable for the creation of the tunnels between the remote Clusters. The purpose of the tunnels is twofold. First, they provide a secure means for inter-Cluster communication by shielding the intra-PN communication from the outside world. Secondly, these tunnels will be established and maintained dynamically, efficiently dealing with Cluster mobility.

Establishing and maintaining these tunnels dynamically, consumes resources (processing, battery power) and it could be questioned if this burden should be placed on the Gateway Nodes in the Cluster, which are often mobile and battery-powered. In PN-capable infrastructure, Edge Routers can provide PN services supporting this functionality. Edge Routers are nodes in the access parts of the infrastructure probably owned and managed by a network or service provider, which communicate with Gateway Nodes. This means that, on behalf of a Cluster, an Edge Router can communicate with the PN Agent(s) and could take care of the tunnel establishment and management if the user desires so. Thus, the Edge Router can relieve the Gateway Nodes, allowing them to reduce their power consumption. In case no Edge Routers are present, remote Clusters can still find each other though registration with the PN Agent, and can set up secure tunnels between their Gateway Nodes.

The PN Agent maintains a table of registered Clusters and the IP addresses of the Edge Routers that are serving as their ingress and egress tunnel endpoints. It partakes in PN establishment, maintenance and management by interacting with a naming system, addressing and routing, PN management, mobility management and the security framework. In the described scenario of Figure 5, the PN Agent is integrated in a naming system used to address PN constituents using names. The naming system is a distributed peer to peer overlay network containing name resolvers combined with a service discovery framework.

Figure 5 depicts a cluster (here the P-PAN) connecting to another remote PN cluster:

1. The P-PAN registers itself with the PN Agent. For example, in Figure 5, the P-PAN Gateway Node passes its Cluster name [PN=PN1][Cluster=Gateway of P-PAN]) to the provider Edge Router after discovery of (and establishment of trust with) this Edge Router. The provider Edge Router concatenates its IP address with the Cluster name and transmits the resulting name record to the PN Agent.
2. Upon successful registration, the PN Agent interacts with the tunnel (overlay network) management system to provide the overlay network membership information and define the overlay-Identifier. The PN Agent updates the overlay membership information upon new cluster registrations by communicating with overlay management.
3. Tunnel or overlay management sends the overlay membership data to the Edge Router involved in the overlay. The Edge Router will install virtual routing tables for the new PN and a tunnel endpoint for the PN using the PN prefix.
4. The PN Agent sends the overlay membership information to the Edge Router, informing about registration of other Clusters belonging to the same overlay.
5. The Edge Routers, associated to the PN desired/requested overlay, can now establish dynamic tunnels across the backbone to connect the Clusters.
6. The Gateway Node sends a routing update containing the list of Cluster Nodes to the Edge Router. This table acts as a proactive routing table for the specific overlay currently being established.
7. The routing information provided by the gateway is forwarded to the remote Edge Routers that have clusters of the same PN connected to them, and exchange of their proactive routing tables takes place.

For PN maintenance, in the proactive PN solution, once the Cluster registration has been completed, the Gateway Nodes have to inform the Edge Router about each change

TABLE 2: IMPLEMENTED COMPONENTS FOR MAGNET PROTOTYPE

Name of the component	*Implementation framework*	*Interface(s) towards other components*	*MAGNET entities implementing component*
Neighboring	Linux kernel module	Imprinting, UCL, Routing	Personal Node
UCL	Linux kernel module	Neighboring	Personal Node
Routing	Click modular router	Neighboring, AA, Edge Router, PN Agent	Personal Node, Gateway, Edge router
SMN	UPnP implementation INS Twine implementation UPnP – INS translation	SMN Election	SAN
PN Agent (Naming system)	INS Twine implementation	Edge Router, Routing	Edge router
Edge Router	Click modular router	Routing, PN Agent	Edge router
SMN Election	Linux daemon	SMN	SAN
Address Autoconfiguration (AA)	Linux daemon	Imprinting, Routing	Personal Node
Imprinting	Bluetooth SDP and L2CAP API IEEE 802.11 WPA	Neighbouring, AA	Personal Node

in the composition of the Cluster. To this end, the intra-Cluster routing protocol has been extended with additional routing protocol messages (called Cluster update messages) that are exchanged between the Gateway Node and the Edge Router upon changes in the Cluster composition.

Every time a Node leaves or joins a Cluster, each Node that is part of that Cluster removes or adds a new destination to its intra-Cluster routing table. This action

triggers the Gateway Node of the Cluster to send a Cluster Update message to the Edge Router

As already explained, when a Cluster connects to an Edge Router through a Gateway Node, a virtual router instance will be created in the Edge Router for that PN. Each time the composition of the Cluster changes, the Gateway Node communicates this information to the Edge Router, which will update its virtual routing table. Of course, the Edge Router not only has to update its own virtual routing table, but also has to forward the routing update to the remote Edge Routers (i.e. Edge Routers that also have Clusters of the same PN connected to them), so they can update their virtual routing tables. The end result of the PN-wide routing process is that each Edge Router contains in its virtual routing table the list of all PN Nodes together with the IPSec tunnel through which they can be reached. This way, the PN communications are always up to date and routes to any node in the PN are always ready to be used.

Note that such a set of solutions is only possible if key components such as edge routers and naming systems are introduced in the overall architecture and if interoperability with legacy networks is addressed. Even if the components are readily available within MAGNET, additional effort is still on going within the project to ensure interoperability and interfacing with existing infrastructures.

Proof-of-concept prototype

It is important to note that the solutions proposed in this document have been implemented on real platforms in order to provide a proof-of-concept prototype that demonstrates the feasibility of the PN concept proposed. Table 2 summarizes the main components integrated in the prototype as well as the frameworks on which the implementation has been performed.

Conclusion

In the last two years of its operation, MAGNET has defined a secure and user centric personal network architecture (PN) based on trust between personal devices and components. The proposed architecture can achieve secure service and context discovery and networking of devices, nodes, services and applications inside and outside of the personal network. The present document describes the functional components of the secure PN architecture.

In order to reflect the possible challenges and have a more precise notion of the technical problems that may arise in different communication settings, in terms of security, routing, network establishment and maintenance, mobility etc., the network architecture has been introduced following a layered approach where three abstraction levels have been identified.

These key functions and the conceptual secure PN architecture have been cast into a connectivity abstraction level (regrouping air interfaces, MAC and DLC), a network abstraction level (addressing higher layer connectivity in the P-PAN when needed and networking within the PN), and a service abstraction level responsible for combined naming resolution, service and context discovery.

The MAGNET architecture has put forward a novel concept where both the architecture and protocols are relying on the notion of long term and short term trust relationships. The long term trust, which can be perceived as permanent trust, is used to establish a strong security association or relationship between the nodes and devices of the PN. For providing connectivity over heterogeneous radio domains composing the P-PAN, a Universal Convergence Layer solution has been adopted. The addressing in the PN network is selected to be flat and data is forwarded using an ad hoc routing protocol with multi-interface and gateway support. Furthermore the project has identified several solutions for PN establishment and maintenance such as PN agent based solution. Less interest has been put on the mechanisms for providing the user with access to both private and public services. Within MAGNET, a specific MAGNET Service Discovery Architecture and Protocol has been developed that provides the mechanism and functionalities for service discovery within and around the PN.

Future Lines

Even though a clear PN architecture and concepts have been summarized in this document, it is important to notice that the present PN architecture in MAGNET can still evolve and improve. MAGNET has adopted very flexible frameworks not only at the radio interfaces level but also in the networking sector where open programmable frameworks are envisaged to empower the end users with flexibility and some control of their own security and connectivity. The on going research activities in the community will affect the detailed future architecture and possibly contribute towards improved implementation of the PN concepts and the pilot services. The solutions achieved so far sustain also the MAGNET in depth research program focussed on evolutionary paths for future generation personal networks and services.

In MAGNET, two Agent based architectures are investigated: The NEMO solution for network mobility and the proactive PN Agent with Edge Nodes, discussed in this document, whose objective is to provide added value services and potentially supplement more de facto standard approaches. A future research line would be to further analyze and compare both approaches and to come up with the design recommendations.

Finally, it is important to note that, in this document, only communication between personal nodes has been covered. However, a PN cannot exist in isolation, but needs to interact with other PNs as well as PN-unaware foreign nodes and devices, including legacy devices. The architecture presented offers enough flexibility to allow solutions dealing with these challenges to be part of it. Nevertheless, more effort will be put on this topic to extend the current architecture and solutions.

ACKNOWLEDGMENT

This paper describes work undertaken in the context of the FP6-IST-IP-507102 'My personal Adaptive Global Net' IST-MAGNET project. MAGNET is a worldwide R&D project within Mobile & Wireless Communication beyond 3G. MAGNET will introduce new technologies, systems, and applications that are on the same time user-centric and secure. MAGNET will develop user-centric business model concepts for secure Personal Networks in multi-network, multi-device, and multi-user environments. MAGNET has 37 partners from 17 countries, -highly acknowledged Industrial Partners, Universities, and Research Centers.

Please visit: www.ist-magnet.org

The authors would like to acknowledge the collaboration of their colleagues from the MAGNET Consortium.

REFERENCES

[1] I.G. Niemegeers and S. Heemstra de Groot, "From Personal Area Networks to Personal Networks: A user oriented approach", Journal on Wireless and Personal Communications 22 (2002), 175-186.

[2] I. Niemegeers and S. Heemstra de Groot, "Personal networks: Ad hoc distributed personal environments," Med-HocNet, IFIP Conference on Ad-Hoc Networks, September 2002.

[3] FP6-IST-IP-507102 'My personal Adaptive Global Net' IST-MAGNET project. www.ist-magnet.org

[4] E. Gustafsson and A. Jonsson, "Always best connected," IEEE Wireless Communications, vol. 10 , no. 1 , pp. 49-55, 2003.

[5] IEEE 802.15 Working Group for WPAN, http://www.ieee802.org/15/

[6] IETF Mobile Ad hoc NETworks (MANET) working group, http://www.ietf.org/html.charters/manet-charter.html

[7] IETF Zero Configuration Networking (Zeroconf) working group, http://www.zeroconf.org/

[8] UPnP™ Forum, www.upnp.org

[9] R.V. Prasad, M. Jacobsson, S. Heemstra de Groot, A. Lo, I. Niemegeers, "Architectures for Intra-Personal Network Communication", In the Third ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH2005), Cologne, Germany, September 2, 2005.

[10] S. Deering, R. Hinden, "RFC 2460: Internet Protocol, Version 6 (IPv6) Specification", Network Working Group of the Internet Engineering Task Force, December 1998

[11] R. Braden, "RFC 1122: Requirements for Internet Hosts -- Communication Layers", Network Working Group of the Internet Engineering Task Force, October 1989

[12] IST-507102 MAGNET, Deliverable D4.3.2, "Final version of the Network-Level Security Architecture Specification", S. Mirzdeh et al., March 2005.

[13] IST-507102 MAGNET, Deliverable D3.3.2, "MAC/RRM Schemes for WPAN", M. De Sanctis et al., October 2004.

[14] IST-507102 MAGNET, Deliverable D2.2.1, "Resource and Service Discovery: PN Solutions", M. Ghader et al., December 2004.

[15] W. Adjie-Winoto, E. Schwartz, H. Balakrishnan, J. Lilley, "The design and implementation of an intentional naming system", Proc. 17th ACM SOSP, Kiawah Island, SC, Dec. 1999.

[16] R. Hinden, B. Haberman, "RFC 4193: Unique Local IPv6 Unicast Addresses", Network Working Group of the Internet Engineering Task Force, October 2005

[17] R. Hinden, S. Deering, "Internet Protocol Version 6 (IPv6) Addressing Architecture", IETF RFC 3513, April 2003.

[18] J. Lipman, P. Boustead, J. Chicharo, "Reliable Optimised Flooding in Ad hoc Networks". In proceedings of the IEEE 6th CAS Symposium on Emerging Technologies: Frontiers of Mobile and Wireless Communication, Shanghai, China, May 2004.

[19] M. Jacobsson, C. Guo, I. Niemegeers, "A Flooding Protocol for MANETs with Self-Pruning and Prioritized Retransmissions", In the International Workshop on Localized Communication and Topology Protocols for Ad hoc Networks (LOCAN2005), Washington, DC, USA, November 7, 2005.

Luis Muñoz is Associate Professor at the University of Cantabria. He received the Telecommunications Engineering Degree by the Telecommunications Engineering School of Barcelona, Polytechnical University of Cataluña (UPC), Spain, in 1990 and the Ph.D. also by the UPC in 1995.
He joined the University of Cantabria in 1990 first as Assistant Professor of the Electronics Department and from 1996 as Lecturer of the Communications Engineering Department. He is head of the Data Transmission and Mobile Networks group belonging to DiCOM. He started to work in the field of Data Transmission and Mobile Networks since 1990, first in topics related with modulation, equalisation techniques and channel coding; later he begun to work in mobile networks with voice and data integration, designing and carrying out projects as TETRA for power utilities, security systems and telecontrol with real time needs. He has participated in projects of the IV Framework of the E.U. R&D Programme, such as ACTS and at present he is participating in the V Framework, IST. His group has strong relationships with the Spanish Telecom operators and manufacturers companies belonging to these sectors.
In parallel to this activity Dr Luis Muñoz serves as consultant of different companies.

Luis Sánchez received the Telecommunications Engineering Degree by the Telecommunications Engineering School of Santander, University of Cantabria (UC), Spain, in 2002. Since 2001 he has been a researcher at the Communications Engineering Department on that university, where he is also pursuing his PhD. His research interest focus is on: 1) Mobile communications, performance analysis and MAC/LLC protocol design for wireless networks; 2) Self-configuration in ad hoc networks; and 3) Service discovery in Personal Networks.

Jorge Lanza received a degree in Telecommunications Engineering from the University of Cantabria (UC), Spain, in 2000. Since then he has been a researcher at the Data Transmission and Mobile Networks group of that university, where he is currently working toward a PhD. in communications engineering. His research activities focuses on ad hoc networks over wireless technologies, specially making emphasis on protocol design and performance analysis of TCP/IP protocols over real test-beds, such as muti-hop wireless environments. As a member of the Technical Observatory for Smart Cards at the University of Cantabria (OTTIUC), he also works with highly regarded manufacturers, banking entities and mobile operators acquiring experience in smartcard technology, highlighting a patent request concerning security and user authentication mechanisms through mobile phones. Current research in combined mobility and security for the wireless Internet is been carried out based on the merging of wireless technologies and smartcards for current and next generation networks.

Mikko Alutoin received his M.Sc. from Helsinki University of Technology (HUT) in 2000. His research area includes e.g. TCP/IP networking protocols and routing and switching architectures. He has participated in several national and international projects such as EU-IST CONTEXT. He is currently PhD student at HUT.

Sami Lehtonen received his Masters Degree from Lappeenranta University of Technology and he has been working at VTT since 1999. He has been working in several international projects concerning security, programmable networks and overlay networks.

Djamal Zeghlache graduated from SMU in Dallas, Texas in 1987 with a Ph. D. in Electrical Engineering and

joined the same year Cleveland State University as an Assistant Professor. In 1992 he joined the "Institut National des Télécommunications" (Evry, France) where he currently heads the Wireless Networks and Multimedia Services Department. Professor Zeghlache has sustained research and scholarly activities in the field of wireless networks and services with actual emphasis on awareness, cooperation and adaptation in wireless and personal networks.

Marc Girod-Genet graduated from Université de Versailles in 2000 with a doctoral Degree in Computer Science and joined INT as research scientists to work on European and National research and development projects until 2004. He also holds a Master's degree for the Stevens Institute of Technology, USA. He was involved in the following National projects: DILAN and MMQoS. At the European level he played a key role for INT-GET in MONASIDRE and currently doing the same in FP6 IP project MAGNET. In 2004 he joined INT as a full time Associate Professor. His research interests include: optimization and learning in telecommunications and computer networks, policy based management and control, AA frameworks for networks and services, context and service discovery management and provisioning.

Wajdi Louati received the MS Degree in Computer Science (2003) from Pierre et Marie Curie University (Paris, France). Currently, he is a Ph. D. student at "Institut National des Télécommunications" (Evry, France) in the wireless networks and multimedia services department. His main research interests include programmable routers and networks and overlay networks with a current focus on Personal Networks.

Jeroen Hoebeke was born in Ghent, Belgium in 1979. In 2002, he received the Masters degree in engineering (Computer Science) from the University of Ghent. In August 2002, he joined the Broadband Communications Networks Group where he is currently working as a research assistant of the Fund for Scientific Research Flanders. His PhD research includes the development of adaptive routing protocol techniques for mobile ad hoc networks, self-organization and routing in personal networks and ad hoc overlay networks. His main research interests are in ad hoc wireless communications and, more generally, in broadband wireless communications.

Ingrid Moerman was born in Gent, Belgium, in 1965. She received the degree in Electro-technical Engineering and the Ph.D degree from the Ghent University, Gent, Belgium in 1987 and 1992, respectively. Since 1987, she has been with the Interuniversity Micro-Electronics Centre (IMEC) at the Department of Information Technology (INTEC) of the Ghent University, where she conducted research in the field of optoelectronics. In 1997, she became a permanent member of the Research Staff at IMEC. Since 2000 she is part-time professor at the Ghent University. Since 2001 she has switched her research domain to broadband communication networks. She is currently involved in the research and education on broadband mobile & wireless communication networks and on multimedia over IP. Her main research interests related to mobile & wireless communication networks are: adaptive QoS routing in wireless ad hoc networks, personal networks, body area networks, wireless mesh networks, sensor and actuator networks, wireless access to vehicles (high bandwidth & driving speed), protocol boosting on wireless links, QoS support in wireless networks. She is author or co-author of more than 300 publications in the field of optoelectronics and communication networks.

Gerry Holderbeke was born in Zottegem, Belgium in 1982. He graduated in Informatics at the University of Ghent in 2004. In August 2004, he joined the Broadband Communications Networks Group where he is currently working as a project developer. His research currently includes the development of an emulator for mobile ad hoc networks. His main research interests are in ad hoc networks and broadband wireless communications and involve routing, addressing and more generally, an approved communication within mobile ad hoc networks. Within the European MAGNET project, he is actively involved in the development of a network architecture for Personal Networks, with a prime focus on the implementation of the routing architecture.

Majid Ghader, MSc., BSc.: is a research fellow at the Centre for Communication Systems Research (CCSR), University of Surrey. He has worked as a Network Expert, IT Consultant, and Software Developer in several industrial companies and organisations. He moved to University of Surrey in 2001. Since then, he has been involved in design and management of Wireless Network Test bed. His research is on Service discovery, provision and general service platforms for wireless environments. Majid is registered as a PhD candidate in Mobile Communication Systems.

Martin Jacobsson graduated in Computer Science at the University of Linköping, Sweden in 2002. In 2003, he joined the Wireless and Mobile Communications group led by professor Niemegeers in Delft University of Technology as a researcher. His PhD research includes self-organization techniques in combination with infrastructure-based networks for personal networks. His main research interests are autoconfiguration and self-organization in wireless mobile ad hoc and hybrid networks.

WIRELESS WORLD RESEARCH FORUM

WWRF#15 meeting

"Convergence and Seamless Mobility"

8 – 9 December 2005

Paris, France.

Detailed Program

Overview

	Thursday 8 December 2005		Friday 9 December 2005
9:00	Opening Plenary Session	9:00	Panel on Digital Convergence
10:45	*Coffee Break*	10:45	*Coffee Break*
11:00	Chair and Vice Chair election 1st WG session	11:00	3rd WG session
12:45	*Lunch*	12:45	*Lunch*
13:45	1st SIG session	13:45	2nd SIG session
15:30	*Coffee Break*	15:30	*Coffee Break*
15:45	2nd WG session	15:45	4th WG session
17:00	Convergence session		
18:00	General Assembly election		17h30
	20h00 Welcome Diner		

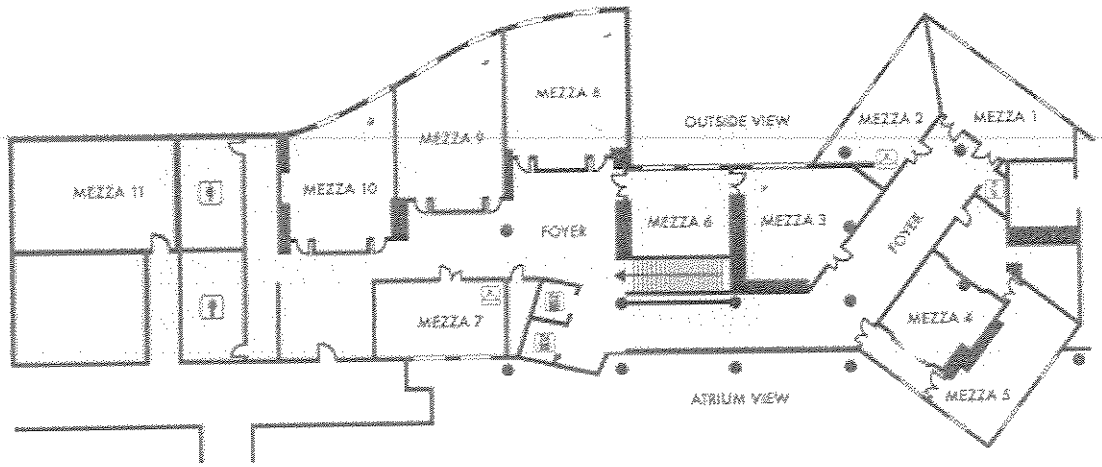
Meeting Room Assignments

December 8

	Grand Apogee	Apogee 2	Apogee 4	Apogee 6	Mezza 8	Mezza 9	Mezza 10
9h00-10h 45	Plenary						
11h00-12h45		WG 3	WG 1	WG 6	WG 4	WG 2	WG 5
12h45-13h45	**Lunch at Café Mirage**						
13h45-15h30		SIG 3		SIG 2		SIG 1	
15h45-17h00		WG 3	WG 1	WG 6	WG 4	WG 2	WG
17h00-18h00	Plenary						
18h00-20h00	GA						
20h	**Welcome Diner at Café Mirage**						

December 9

	Grand Apogee	Apogee 2	Apogee 4	Apogee 6	Mezza 8	Mezza 9	Mezza 10
9h00-10h 45	Plenary						
11h00-12h45		WG 3	WG 1	WG 6	WG 4	WG 2	WG 5
12h45-13h45	**Lunch at Café Mirage**						
13h45-15h30		SIG 3	SIG 4	SIG 2		SIG 1	
15h45-17h00		WG 3	WG 1	WG 6	WG 4	WG 2	WG 5
17h00-17h30		WG4 + WG5					



GROUND FLOOR LEVEL
RECEPTION
BUSINESS CENTER
MEZZANINE LEVEL SOUTH
ATRIUM
JUPITER
SATURNE
APOGÉE 1
APOGÉE 3
APOGÉE 5
GRAND APOGÉE
FOYER
APOGÉE 2
APOGÉE 4
APOGÉE 6
APOGÉE 7
APOGÉE (2+4+6)
ENTRÉE CONVENTION
PARKING

Detailed Session Agendas

Plenary Session – Part 1

Day 1 – Thursday 8th 09:00 – 10:45

GRAND APOGEE

Session Chair: Brigitte Cardinaël		
Time	**Title**	**Presenter**
09:00	Welcome to WWRF15	Brigitte Cardinaël & Paul Friedel
09:15	WWRF system requirements and concepts	**Mikko A. Uusitalo,** Chairman of the Wireless World Research Forum Head of International Cooperation, Nokia Research Center
09:45	Keynote #2 – title TBD	**Paul Friedel** , Research Director , France Telecom Research and Developpment
10:15	Keynote #3 – title TBD	**Gary Grube,** Vice President and Director of Wireless Applications Research, Motorola Labs
10:45	**Coffee Break**	

Plenary Session – Part 2

Day 1 – Thursday 8th 17:00 – 18:00

GRAND APOGEE

Session Chair: Andy Jeffries		
Time	**Title**	**Presenter**
17:00	Keynote #4 – title TBD	**Walter Tuttlebee**, Mobile VCE chair
17:30	Keynote $5 – title TBD	**Phil Hendrix,** Director, Institute for Mobile Markets Research (IMMR)

Plenary Session part 3

Day 2 – Friday 9th 09:00 – 10:45

GRAND APOGEE

Moderator: TBD		
Time	**Title**	**Panelists**
09:00	Panel topic: "Digital Convergence"	France Telecom, Warner Music, ARCEP
10:15	Keynote #6 – title TBD	**Joao Da Silva,** Director Network and Communication Technologies, European Commission
10:45	**Coffee Break**	

WG /SIG Sessions

WG1 – Human Perspective and Service Concepts

WG1 is focused on discovering and promoting research areas that strive to understand end-users' actual needs for future wireless systems and how users will interact with devices, systems and applications in the wireless world

WG1 Session 1		
Day 1 – Thursday 8th December 10:00 – 13:45		**Session Chair: M. Angela Sasse**
Time	**Title**	**Presenter**
11^{00}-11^{30}	Election of Chair and Vice Chair for WG1 for 2006	
11^{30}-11^{50}	Introduction: WG1 Status	M. Angela Sasse (UCL)
11^{50}-12^{20}	Conflicts of convergence: The mobile as a schizophrenic device	Carl Adams (University of Portsmouth)
12^{20}- 12^{45}	CoPE methodology of the Vision Book of NGMC Forum	Frank Rhee,Gyung-Chul Sihn, Dae-Sik Kim (ETRI)
12^{45}-13^{45}	**Lunch**	
13^{45}-15^{30}	*SIG Sessions*	
15:30	**Coffee Break**	

WG1 Session 2: WG1/SIG2 Joint Session		
Day 1 – Thursday 8th December 15:45 – 17:00		**Session Chairs: M. Angela Sasse, Mario Hoffmann**
Time	**Title**	**Presenter**
15^{45}-16^{00}	New White Paper Launch: Usable Security for Services and Applications B3G	M. Angela Sasse (UCL) & Mario Hoffman (FHG SIT)
16^{00}-16^{30}		Stewart Kowalski
16^{30}-17^{00}	People and Security: Implications for Future Mobile Services & Applications	M. Angela Sasse (UCL)

WG1 Sessions 3 & 4		
Day 2 – Friday 9th December 11:00 – 17:30		**Session Chair: Mikael Anneroth**
Time	**Title**	**Presenter**
11^{00}-11^{30}	A Federated Services Concept for Advanced Personalization	Heinz-Josef Eikerling (Siemens)
11^{30}-12^{00}	User-Centred Design in the Context of Large and Distributed Projects: Case MobiLife	Esko Kurvinen, Andrew Aftelak (Motorola) and Annakaisa Häyrynen
12-12^{45}	Invited Presentation: Convergence	Phil Hendrix Director, Institute for Mobile Markets Research (immr) (IMMR)
12^{45}-13^{45}	**Lunch**	
13^{45}-15^{30}	*SIG Sessions*	
15:30	**Coffee Break**	
15^{45}-17^{00}	WG 1 White Paper Working Teams	

WG2 - Service Architecture

WG2 focuses on service support platform architectures and enabling technologies for future wireless communication systems. The WG2 follows the WWRF approach to regard the user in a ubiquitous communication environment the driving force for future mobile systems. Based on the assumption of an IP-based, always connected world, WG2 investigates service support environments, allowing to provide individual users with user-centric, ubiquitous and context-aware services and applications. The working group gathers inputs and views from industry and academia and synthesizes these views to influence future visions and research priorities and to share results across the Forum.

WG2 Sessions 1 & 2		
Day 1 – Thursday 8th December 10:00 – 16:45		**Session Chairs: Stefan Arbanowski, Wolfgang Kellerer**
Time	**Title**	**Presenter**
11^{00}-11^{30}	Election of Chair and Vice Chair for WG2 for 2006	
11^{30}-11^{50}	Introduction, current status of WG2, achievements in 2005, further plan	Stefan Arbanowski (Fraunhofer FOKUS), Wolfgang Kellerer (DoCoMo Euro-Labs)
11^{50}-12^{45}	The Simplicity System and its Demonstrator	G. Bartolomeo, N. Blefari-Melazzi, S. Salsano (U. Rome); J. Hamard, C. Noda (DoCoMo Euro-Labs)
12^{45}-13^{45}	**Lunch**	
13^{45}-15^{30}	*SIG Sessions*	
15:30	**Coffee Break**	
15^{45}-16^{10}	Applying Semantic Web Technologies for mobile communications	Josef Noll, Erik Lillevold (UniK, Norway)
16^{10}-16^{35}	URBAN NETSPOT testing environment for next generation services	Inés Vidal, Fernando Andreu (Euskaltel)
16^{35}-17^{00}	Mobile Content Provisioning – Major Issues	S.R. Subramanya (LGE Mobile Research), Byung K. Yi, (LGE Electronics)

WG2 Sessions 3 & 4		
Day 2 – Friday 9th December 11:00 – 17:30		**Session Chairs: Stefan Arbanowski, Wolfgang Kellerer**
Time	**Title**	**Presenter**
11^{00}-11^{25}	Privacy Management Using Policy Decision and Enforcement - Single User Privacy and Sharing Data among a Group in a Distributed System	G. Schultz, J. Hjelm, S. Holtmanns and R. v Eijk (Ericsson Research)
11^{25}-11^{50}	Service architecture enabling advanced mobile applications from business model perspective	Ulla Killström (Elisa Corporation), Bernd Mrohs, Stephan Steglich, (Fraunhofer FOKUS)
11^{50}-12^{15}	Learning Context for Personalisation of Ambient Awareness for Communication and Service Adaptation and Propagation,	Adrian Flanagan (Nokia Research Center)
12^{15}-12^{40}	Profile Management for next generation mobile service Platform	Don-sung Oh (ETRI)

12^{45}-13^{45}	**Lunch**	
13^{45}-15^{30}	*SIG Sessions*	
15:30	**Coffee Break**	
15^{45}-16^{10}	DRAGO: Mobile Service Architecture for Access and Management of Context-Aware "A La Carte" Audiovisual Content in the Tourism and Leisure Industry	J. C. Guerri, A. Pajares, Á. Belda (iTEAM – Universidad Politécnica de Valencia), O. Lazaro (Innovalia Association), J.M. Losada (CBT Comunicación & Multimedia)
16^{10}-16^{35}	Flexible Multicast Service Provision for 4G	Diogo Gomes (Instituto de Telecomunicações) Rui Aguiar, Amardeo Sarma, Karl Jonas
16^{35}-17^{00}	Achieving Architecture Validation Purposes through Model Driven Approaches	M.F. Menaï, G. Fromentoux, G. Champion and B. Cardinaël, (France Telecom), D.Gaïti, M. Lemercier (University of Technology of Troyes - France)
17^{00}-17^{25}	Location-based Service Discovery System for Next-Generation IMS in Beyond 3G Converged Networks	Geng-Sheng (G.S.) Kuo (National Chengchi University), Tian Wu, L. Wang, Xu Zhang, L. Mu, Gang Li (Beijing University of Posts and Telecommunications)

WG3 - Co-operative and Ad-Hoc Networks

WG3 is focused on studying co-operative and ad hoc networks as an integral and evolving part of the future communication infrastructure taking in account both wireless and fixed aspects. WG3 aims at defining meaningful scenarios and a framework for ad hoc and sensor networks in the WWRF and B3G context especially taking in account (civilian) industry scenarios. We further strive for the identification of a framework, architecture and components for co-operative networks. In general WG3 aims for an understanding of the next generation network paradigms of B3G and all-IP scenarios.

WG3 Sessions 1 & 2		
Day 1 – Thursday 8th December 10:00 – 16:45		**Session Chairs: Petri Mahönen**
Time	**Title**	**Presenter**
11^{00}-11^{30}	Election of Chair and Vice Chair for WG3 for 2006	
11^{35}-11^{55}	Energy-efficient ARQ Protocol for Unbalanced Multi-hop Routes in Hybrid Networks	Xu, Yiling, Samsung Korea
11^{55}-12^{20}	Adaptive H.264 Packet Size Selection for 802.11 Inter-Vehicular Ad Hoc Networks	Enrico Masala, Polytechnico Torino
12^{20}-12^{45}	Dynamic Gateway for Ad-hoc Networks	Kaouthar Sethom, INT
12^{45}-13^{45}	**Lunch**	
13^{45}-15^{30}	*SIG Sessions*	
15:30	**Coffee Break**	
15^{45}-16^{05}	Scalable reliable multicast transport for heterogeneous mobile IPv6 environment	Ilka Miloucheva
16^{05}-16^{30}	An Overlay Internetworking Architecture for Ambient Networks	Anders Eriksson
16^{30}-17^{00}	Securing Network Attachment and Compensation	Seppo Heikkinen,Tampere Uni

WG3 Sessions 3 & 4		
Day 2 – Friday 9th December 11:00 – 17:30		**Session Chair: Petri Mahönen**
Time	**Title**	**Presenter**
11^{00}-11^{30}	**Overall White Paper discussion**	all
11^{30}-11^{50}	**White Presentation on Wireless Sensor Networks**	J. Riihijärvi, RWTH Aachen University
11^{50}-12^{15}	Network Composition	Martin Johnsson, Ericsson
12^{15}-12^{45}	Ambient Networks challenges and results	Johan Nielsen (ed.), Ericsson
12^{45}-13^{45}	**Lunch**	
13^{45}-15^{30}	*SIG Sessions*	
15:30	**Coffee Break**	
15^{45}-16^{05}	Broadcast Meets Mobile	Paul Pangalos ,KCL
16^{05}-16^{30}	Multi-Radio Access in Ambient Networks	George Koudouridis , TeliaSonera
16^{30}-17^{00}	Achieving Inter-RAN Cooperation: An Architecture Proposal	Vaia Sdralia, Samsung UK

WG4 - New Air Interfaces, Relay based Systems and Smart Antennas

WG4 focuses on air interfaces, and smart antenna and relay network enhancements, in metropolitan and wide-area environments; i.e. wireless MAN and WAN point-to-multipoint, unicast, multicast and broadcast systems, with or without mobility. The beyond-3G systems under consideration are characterized by aggregate bit rates in the 100 Mb/s range or higher, high mobility, high user capacity and ubiquity, and coexistence with complementary services sharing the same or adjacent spectrum. Typical distances between mobile terminals and access points are greater than 100 m, although communication may be facilitated by a relay network with shorter inter-relay distances.

Session 1 11:00-12:45 Day 1 ELECTION AND WG4 POSTERS		
11:00-11:10	Welcome & Overview	David Falconer (Carleton University, Canada)
11:10-11:40	WG4 election of Chair and Vice-Chair for 2006	
11:40-12:45	**WG4 POSTERS**	
Low Complexity Spatial Multiplexing Scheme over Correlated Channels using Feedback		Kothapalli[2] V. Srinivas[1] J. Klutto Milleth[1] K. Giridhar[2] ,R. D. Koilpillai[2] [1]Centre of Excellence in Wireless Technology Telecom. & Computer Networks Group CSD/ESB, Opp. Media Lab Asia [2]Department of Electrical Engineering Indian Institute of Technology, Madras Telecommunications and Computer Networks (TeNeT) Group Department of Electrical Engineering Indian Institute of Technology, Madras
Controlling Array Gain Using Partial Channel Feedback in Linearly Decodable STF Codes		V. Babu[1], B. Ramamurthy[2], K. Gridhar[2] [1]Centre of Excellence in Wireless Technology Telecom. & Computer Networks Group CSD/ESB, Opp. Media Lab Asia [2]Telecommunications and Computer Networks (TeNeT) Group Department of Electrical Engineering Indian Institute of Technology, Madras
Space Division Multiplexing/Space Division Multiple Access Unitary Precoded MIMO		Cheol Mun*, Do-Youn Kim**, Jong-Gwan Yook**, Jin-Kyu Han***, and Hyeon-Woo Lee*** *Dept. of Electronic Communications Eng.,Chungju Nat'l Univ., Korea, **Dept. of Electrical & Electronic Eng.,Yonsei Univ., Korea, ***Telecomm. R&D Center, Samsung Electronics
Performance of LDPC Codes with 16QAM for Unequal Error Protection		Soyeon Kim, Kihyoung Cho, Minseok Oh. Mobile Communication Technology Research Lab. LG Electronics, Korea
Overview of WINNER Channel Modeling Activities		Tommi Jämsä, Juha Meinilä, Pekka Kyösti, Elektrobit Testing Ltd. Daniel S. Baum, Swiss Federal Institute of Technology (ETH) Zürich Hassan El-Sallabi, Helsinki University of Technology Terhi Rautiainen, Nokia Research Center Christian Schneider, Marko Milojević, Technische Universität Ilmenau Per Zetterberg, Royal Institute of Technology (KTH), Stockholm
Optimal Design of Subband-Frame Size and Modulation Mode for Adaptive OFDM-TDD based Mobile System		Jung-Gon Kim Dept. of Electronics Engineering, Korea Polytechnic University, Kil-Ho Shin Telecommunications Research Center Samsung Electronics, Co. Ltd.

PARAFAC Models for Hybrid MIMO Systems: Joint Channel Estimation and Detection	A.Almeida, G. Favier, J. Mota, Charles Casimiro Cavalcante, Campus do Pici, Brazil
Carrier frequency assignment for the fixed relay based architecture for a DS-CDMA based mobile cellular system	Y.C Chow and D. R. Basgeet Telecommunications Research Laboratory, Toshiba Research Europe Limited
Relay Configurations for Spatial Multiplexing MIMO Channels	Yijia Fan (1), John Thompson (1) and Mark Naden (2)

SIG2 - Security and Trust

The subject matter scope of the special-interest group includes all areas relevant to the security and trustworthiness of future wireless systems and the applications and services that are used over them.

Sig2 Session 1		
Day 1 – Thursday 8th December 13:50 – 16:15		Session Chair:
Time	Title	Presenter
13^{50}-14^{10}	Anonymous Network Access using a Secure Digital Marketplace	Alisdair McDiarmid, James Irvine (Institute for Communications and Signal Processing, University of Strathclyde)
14^{10}-14^{30}	Distributed security mechanisms for Personal Networks"	Dimitris M. Kyriazanos et.al. - Institute of Communication and Computer Systems (ICCS), National Technical University of Athens (NTUA)
14^{30}-14^{50}	Security Considerations for Converged Networks	Miroslav Zivkovic and Harold Teunissen (Lucent Technologies – Bell Labs Europe)
14^{50}-15^{10}	Identity Management and Privacy issues in DAIDALOS pervasive environment	Jan Porekar (SETCCE, Slovenia)
15^{10}-15^{30}	User Authentication to Services in Converging Mobile and Fixed Networks	Silke Holtmanns (Nokia Research Center)

Sig2 Session 2		
Day 2 – Friday 9th December 13:50 – 15:30		Session Chair:
Time	Title	Presenter
13^{50}-14^{10}	SIM-card enabled Seamless Access in Mobile and Broadband Access Networks	Josef Noll, Juan Carlos Lopez Calvet (UniK - University Graduate Centre, N-2027 Kjeller, Telenor R&D, N-1331 Fornebu, Norway)
14^{10}-14^{30}	"Long-term trust for heterogeneous wireless networks	Khaled Masmoudi, Hossam Afifi (Institut National des Télécommunications, France)
14^{30}-14^{50}	Physical Layer Level Intrinsic Secure Wireless Communications	Lorenzo Mucchi, Luca Simone Ronga, Enrico Del Re - Dept. of Electronics and Telecommunications (CNIT – University of Florence)
14^{50}-15^{10}	Security provisioning in an integrated WLAN/WPAN infrastructure and its impact on the handoff performance	Meng Wang, Michael Georgiades - Centre for Communication Systems Research (University of Surrey)
15^{10}-15^{30}	On Secure Mobile Device Management	Dr. Senthil Sengodan (Nokia, San Diego)

SIG3 - Self-organisation in Wireless World Systems

SIG3 is focused on bringing orderliness in the evolving distributed pervasive wireless communication system via adaptive self-organization. It addresses needs and requirements of self-organization of the wireless systems with minimal human intervention required to allow systems to operate the way they are expected to do. The goal is to develop solutions (concepts, tools, and techniques) for self-organization where human is part of the overall adaptive self-organization system, and thereby to enable new business models for existing and new classes of players, such as "micro operators".

Sig3 Session 1		
Day 1 – Thursday 8th December 13:45 – 15:30		Session Chair: Armadeo Sarma
Time	Title	Presenter
13^{50}-14^{10}	A Proposal for Self-Organising Personal Networks	L. Muñoz
14^{10}-14^{35}	Autoconfiguration and Self-management for Personal Area Networks: a new framework	R. Campos
14^{35}-15^{00}	The Ambient Networks Control Space Architecture	B. Ohlman
15^{00}-15^{30}	Self-configuring Communication Service Module for Wearable Computers	A. Timm-Giel

Sig3 Session 2		
Day 2 – Friday 9th December 13:45 – 14:30		Session Chair: Armadeo Sarma
Time	Title	
13^{45}-14^{10}	Presentation and discussion of new White Paper structure	all
14^{10}-14^{25}	Revision of work plan	all
14^{25}-14^{30}	AOB	all

SIG4 –CONVERGENCE

SIG4 is a new addition to the WWRF structure, and has been introduced to enable WWRF to develop its view of the convergence of the digital industries, which is defined as the bringing together of media and entertainment, broadcasting, telecommunications, information technology and consumer industries in a seamless way to enable selection and combination of services from those available to meet the requirements of a user in any environment

SIG Session 2		
Day 2 – Friday 9th December 13:30 – 15:30		**Session Chair: Andy Jeffries**
Time	**Title**	**Presenter**
13:30	Welcome and review of agenda	
13:35	Remit of SIG4: Convergence	Andy Jeffries, Nortel
13:50	Multiple dimensions of convergence – Outcomes and issues	S. R. Subramanya, LG Mobile Research
14:15	Conflicts of convergence: The mobile as a schizophrenic device	Carl Adams, Portsmouth University
14:40	Broadcast meets mobile	Paul Pangalos, Kings College London
15:05	Discussion	
15:10	Selection of Interim Chair for SIG4	
15:30	**Coffee Break**